No. 22-1744(L)

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

IN RE: MARRIOTT INTERNATIONAL, INC.
CUSTOMER DATA SECURITY BREACH LITIGATION

On Appeal from an order of the United States District Court for the
District of Maryland, Case No. 8:19-md-02879-PWG
Hon. Paul W. Grimm, U.S. District Judge

BRIEF FOR AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION AND ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF PLAINTIFFS-APPELLEES

Cindy A. Cohn
Adam Schwartz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333

Counsel for Electronic Frontier Foundation

Chris Frascella
Megan Iorio
Tom McBrien
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1519 New Hampshire Avenue NW
Washington, DC 20036
(202) 483-1140

Counsel for Electronic Privacy Information Center

Jean Sutton Martin
John A. Yanchunis
Kenya J. Reddy
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 22-1744 Caption: In re: Marriott Int'l, Inc. Customer Data Security Breach Litig.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Electronic Frontier Foundation
(name of party/amicus)

who is Amicus, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐YES ☑NO

2. Does party/amicus have any parent corporations? ☐YES ☑NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐YES ☑NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☐NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☐YES ☑NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: _____ Date: November 22, 2022

Counsel for: Electronic Frontier Foundation

Print to PDF for Filing

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 22-1744 Caption: In re: Marriott Int'l, Inc. Customer Data Security Breach Litig.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Electronic Privacy Information Center
(name of party/amicus)

who is Amicus, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐YES ☑NO

2. Does party/amicus have any parent corporations? ☐YES ☑NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐YES ☑NO
If yes, identify all such owners:

12/01/2019 SCC - 1 -

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☐NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☐YES ☑NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: _____ Date: November 22, 2022

Counsel for: Electronic Privacy Information Center

Print to PDF for Filing

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

STATEMENT OF IDENTITY OF AMICI

The Electronic Frontier Foundation ("EFF") is a nonprofit organization that works to ensure that technology supports freedom, justice, and innovation for all the people of the world. EFF was founded in 1990 and has more than 32,000 members. It advocates before courts and legislatures to protect the privacy of technology users and consumers from corporations that collect and monetize their personal information. EFF has filed numerous amicus briefs that address whether a plaintiff has suffered sufficient injury to enforce a data privacy law. *See, e.g.*, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021); *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016); *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019).

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy issues. EPIC regularly participates as *amicus* in cases concerning individuals' standing to sue for invasions of their privacy rights. *See, e.g.*, Brief for EPIC as *Amicus Curiae* Supporting Respondent, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2016) (No. 13-1339); Brief for EPIC et al. as *Amici Curiae* Supporting Respondent, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (No. 13-1339; Brief for EPIC as *Amici Curiae* Supporting Plaintiffs-Appellees, *Patel v. Facebook, Inc.*, 923 F.3d 1264 (9th Cir. 2019) (arguing that violations of the Illinois Biometric Information Privacy Act confer standing). EPIC has also directly

experienced the impact of *Spokeo* as a litigant when the D.C. Circuit twice applied it to limit the scope of informational standing. *See EPIC v. Presidential Advisory Comm'n on Election Integrity*, 878 F.3d 371, 401–02 (D.C. Cir. 2017); *EPIC v. Dep't of Commerce*, 928 F.3d 95, 103–04 (D.C. Cir. 2019).

The undersigned counsel authored this brief in whole. No party, person, or other entity paid for its preparation or contributed money intended to fund the preparation or submission of the brief.

Both the Appellants and the Appellees have consented to the filing of this brief.

SUMMARY OF THE ARGUMENT

Just as the information collected about consumers is expanding at an unprecedented rate, so too are the risks associated with the collection of such data. As more facets of daily life depend on the data collected in vast corporate databases, a corporation's failure to properly secure and safeguard this data can have serious consequences for many consumers.

As recognized by the Supreme Court's recent decisions in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) and *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), historically, the disclosure of private information has been treated as a sufficiently concrete harm for which individuals may seek redress in federal courts, regardless of whether they have suffered any additional economic harm.

Accordingly, the harm suffered by consumers in data breaches like the one at issue in this case is sufficient to confer each of the Plaintiffs and class members with Article III standing for the claims asserted against Appellants. The classes certified by the District Court—which are far more limited than the number of class members who actually have standing—therefore pose no ascertainability problems requiring reversal of the District Court's certification order.

ARGUMENT

I. DATA BREACHES HAVE BECOME UBIQUITOUS IN THE DIGITAL AGE.

Data breaches are an endemic problem in modern life. A record 1,862 data breaches occurred in 2021, up 68% from the year prior, and far exceeding the previous record of 1,506 breaches in 2017.[1]

Our increasingly digital world has changed the way businesses operate, interact, and transact with consumers. In exchange for goods and services, companies require consumers to provide various forms of information about themselves—names, addresses, dates of birth, Social Security numbers, credit card information, and more. As a result, companies create huge databases of sensitive information about consumers and individuals. The ways in which that information is collected, used, shared, sold, and analyzed create inferences about us that directly impact our everyday lives in ways both visible and invisible.[2]

---

[1] Identity Theft Resource Center, 2021 Annual Data Breach Report, found at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last visited November 14, 2022).

[2] Electronic Frontier Foundation, "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance" at 5, found at https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf (last visited November 14, 2022).

Consumers entrust companies with all of this information with the expectation that those companies—recognizing the extremely sensitive nature of the information they are collecting—will make every effort to secure and safeguard their information. But in reality, data breaches are overwhelmingly attributable to the failure of companies to fix or close known security problems in their systems.[3] The Department of Homeland Security has estimated that 85 percent of data breaches were preventable.[4] More recently, the Internet Society has estimated 95 percent of breaches could have been prevented.[5]

This database-fed ecosystem renders all of us at risk from data breaches while creating a significantly more difficult landscape in which to discover and trace legal causation for the harms we suffer as a result. The information stored in these databases influences critical life events: whether someone is approved for a

[3] Verizon 2022 Data Breach Investigations Report at 40, found at https://www.verizon.com/business/resources/Td0/reports/dbir/2022-data-breach-investigations-report-dbir.pdf (last visited November 14, 2022).

[4] 37 Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, Alert: Top 30 Targeted High Risk Vulnerabilities (2016), found at https://www.us-cert.gov/ncas/alerts/TA15-119A (last visited November 14, 2022). The California Attorney General's Office similarly concluded that many of the hundreds of breaches it studied could have been prevented, or detected and corrected more rapidly, by implementation of its recommended data security controls. See Kamala D. Harris, Attorney General, California Data Breach Report (2016) at 32, found at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (last visited November 14, 2022).

[5] Internet Society, 2018 Cyber Incident & Breach Trends Report at 3, found at https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf (last visited November 14, 2022).

mortgages, hired or fired, provided friendly loan terms, able to rent a home, accepted to an educational institution, verified as themselves to confirm important transactions, or subjected to increased police surveillance and investigation. The injury due to the loss of privacy and control over data that has been negligently disclosed is real and concrete. It has clear impacts on us, even when we cannot easily trace them.

The scale of the problem is difficult to contemplate. The current litigation, impacting approximately 133.7 million individuals, is only the seventh largest data breach of all time, according to a recent news report.[6] In 2021, over 700 million user accounts were breached from LinkedIn.[7] In 2019, over 1 billion pieces of user data were breached from Alibaba.[8] And in 2013, over 3 billion accounts were breached from Yahoo.[9]

The kinds of data stolen in data breaches are extremely sensitive and often

[6] CSO, "The 15 biggest data breaches of the 21st century," found at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited November 14, 2022).
[7] *Id.*
[8] *Id.*
[9] *Id.*

immutable: biometrics,[10] social security numbers,[11] driver's license numbers,[12] credit card numbers,[13] users' physical location history (also known as geolocation

---

[10] Biometrics: U.S. Customs and Border Patrol, "Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot," found at https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf (last visited November 14, 2022); Office of Personnel Management. Notice of Cybersecurity Incidents, found at https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last visited November 14, 2022); Forbes, "New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report." Found at https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=2a3eda9646c6 (last visited November 14, 2022); The Guardian, "Major breach found in biometrics system used by banks, UK police and defence firms," found at https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (last visited November 14, 2022).

[11] Bloomberg Law, "Wells Fargo Sued for Breach That Exposed Social Security Numbers," found at https://news.bloomberglaw.com/privacy-and-data-security/wells-fargo-sued-for-breach-that-exposed-social-security-numbers (last visited November 14, 2022); Tech Crunch, "Hackers stole Social Security numbers in Flagstar data breach affecting 1.5 million customers," found at https://techcrunch.com/2022/06/21/flagstar-bank-social-security-numbers/ (last visited November 14, 2022).

[12] Fox Business, "U-Haul says customer names, driver's license numbers exposed in data breach Driver's license numbers," found at https://www.foxbusiness.com/lifestyle/u-haul-says-some-customer-names-drivers-license-numbers-exposed-data-breach; The Guardian, "Optus tells Victorians whose licences were exposed in data breach to register with roads body," found at https://www.theguardian.com/business/2022/oct/05/optus-tells-victorians-whose-licences-were-exposed-in-data-breach-to-register-with-roads-body ; Tech Crunch, "Geico admits fraudsters stole customers' driver's license numbers for months," found at https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/ (last visited November 14, 2022).

[13] New York Times, "Target to Pay $18.5 Million to 47 States in Security Breach Settlement," found at https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html (last visited November 14, 2022).

information),[14] live feeds from video surveillance cameras,[15] sexual orientation,[16] HIV status,[17] and evidence of romantic infidelity.[18] Here, the data stolen included guests' names, addresses, email addresses, phone numbers, payment card information, passport information, travel destinations, and other information.

Concerningly, personal information disclosed in one data breach can power the next. Verizon estimates that about half of all data breaches involved the misuse of login credentials, which often include personal information such as names and

---

[14] Vox, "This outed priest's story is a warning for everyone about the need for data privacy laws," found at https://www.vox.com/recode/22587248/grindr-app-location-data-outed-priest-jeffrey-burrill-pillar-data-harvesting (last visited November 14, 2022); Tech Crunch, Animoto hack exposes personal information, location data, found at https://techcrunch.com/2018/08/20/animoto-hack-exposes-personal-information-geolocation-data/ (last visited November 14, 2022).

[15] The Verge, "Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, and more," found at https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals (last visited November 14, 2022); Electronic Frontier Foundation, "License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech," found at https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive (last visited November 14, 2022).

[16] Associated Press, "Norway to fine dating app Grindr $11.7M over privacy breach," found at https://apnews.com/article/europe-data-privacy-norway-12d34063d0c20acd0e7a55fc8a6dfe1d (last visited November 14, 2022).

[17] CNN, "HIV status of over 14,000 people leaked online, Singapore authorities say," found at https://www.cnn.com/2019/01/28/health/hiv-status-data-leak-singapore-intl (last visited November 14, 2022).

[18] Wired, "Hackers Finally Post Stolen Ashley Madison Data," found at https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (last visited November 14, 2022).

email addresses.[19] Once an individual's credentials are released (original breach), those credentials can then be used to steal more information about that individual (collateral breach).[20] Thus the loss of data control by an individual due to a single disclosure from companies like Marriott can and does beget additional attacks and disclosures, which can beget still others, in ways that are increasingly difficult to track, much less stop.

For this reason, data breaches like the Marriott data breach cannot be considered individually. Once data has been disclosed from databases such as Marriott's, it is often pooled with other information, some gathered consensually and legally and some gathered from other data breaches or through other illicit means. That pooled information is then used to create inferences about the affected individuals for purposes of targeted advertising, various kinds of risk evaluation, identity theft, and more.[21] Thus, once individuals lose control over personal data that they have entrusted to entities like Appellants, the kinds of harms can grow and

[19] Verizon 2022 Data Breach Investigations Report at 37, found at https://www.verizon.com/business/resources/Td0/reports/dbir/2022-data-breach-investigations-report-dbir.pdf (last visited November 14, 2022).
[20] Verizon 2022 Data Breach Investigations Report at 7, found at https://www.verizon.com/business/resources/Tf3d/reports/dbir/2022-data-breach-investigations-report-dbir.pdf (last visited November 14, 2022).
[21] *See*, *e.g.*, Electronic Frontier Foundation, "Behind the One-Way Mirror: Deep Dive into the Technology of Corporate Surveillance," found at https://www.eff.org/document/behind-one-way-mirror-deep-dive-technology-corporate-surveillance (last visited November 14, 2022).

change in ways that are difficult to predict. Also, it can be onerous, if not impossible, for an ordinary individual to trace these harms and find appropriate redress.

Regardless of the difficulty of tracking one's own information following a data breach, the well-established path from data breaches to harms suffered by individuals is neither speculative nor fanciful. As noted above, once stolen, data is often used to collect more data, re-sold, and recombined with other data. The breach of login credentials has been demonstrated to increase the risk of ransomware attacks, where a person or entity is denied access to their own data unless they pay a ransom.[22] Data breach victims have also been targeted with spam by email and phone.[23] Breaches can also result in identity theft, or in "a significantly increased risk of becoming victims of identity theft in the future."[24] In one recent example, websites used to generate auto insurance quotes were exploited to obtain personal

[22] NordVPN Report, "Dark Web Monitor data: Why are data leaks decreasing?", found at https://nordvpn.com/blog/dark-web-monitor-data-leaks-decreasing/ (last visited on November 14, 2022); SpyCloud, "The Ransomware/Stolen Credentials Connection," found at https://spycloud.com/resource/webinar-ransomware-stolen-credentials-connection/ (last visited November 14, 2022).

[23] TechCruch, "Scammers Now Targeting Anthem Data Breach Victims Via Email and Phone," found at https://techcrunch.com/2015/02/09/scammers-now-targeting-anthem-data-breach-victims-via-email-and-phone/ (last visited November 14, 2022).

[24] Compl., FTC v. Equifax, Inc., No. 1:2019-cv-03297 (N.D. Ga. Jul. 22, 2019) 14, https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf.

data later used to submit fraudulent claims for pandemic and unemployment benefits.[25]

This exposure to the increased risk of identity theft in itself has been demonstrated to cause psychological injury, including anxiety, depression, and PTSD.[26] The psychological injury only increases when identity theft actually occurs. One study by credit reporting giant Equifax found: "identity theft victims may experience similar emotional effects as victims of violent crimes, ranging from anxiety to emotional volatility. … Equifax has interviewed both experts and victims who are dealing with these issues daily."[27] Similarly, according to a 2022 Consumer

---

[25] Industry Letter, New York State Dep't of Financial Services, Cybersecurity Division, *Re: Cyber Fraud Alert* (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.

[26] *See* Danielle Citron and Daniel Solove, "Risk and Anxiety: A Theory of Data Breach Harms", Texas L. Rev. (2018), available at https://scholarship.law.bu.edu/faculty_scholarship/616/ (last visited November 14, 2022); Ido Kilovaty, "Psychological Data Breach Harms," U.N.C. J. of L. & Tech. (2021), available at https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1432&context=ncjolt; Jessica Guynn, *Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes*, USA TODAY (Feb. 24, 2020), found at https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/; Eleanor Dallaway, *#ISC2Congress: Cybercrime Victims Left Depressed and Traumatized*, INFO. SEC. (Sep. 12, 2016), available at https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/.

[27] Equifax, "Lasting impact: The emotional toll of identity theft" (2015), found at https://assets.equifax.com/legacy/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf (last visited November 14, 2022) ("Identity theft

Impact Report by the Identity Theft Resource Center, victims of identity theft suffer psychological injury, including anxiety (80%), depression (49%) and even suicidal thoughts (10%). Victims also report sleep problems (92%), and headaches or other pain (42%).[28]

Another form of harm attendant to data breaches is the need to take affirmative steps to prevent or reduce the chance of future harm, particularly before the actual harms start. These steps, including freezing and unfreezing credit reports,[29]

---

victims often show emotions 'much the way a trauma survivor would respond or somebody who was a victim of a different kind of crime such as a home invasion or assault,' according to Diane Turner, a licensed clinical social worker and certified life coach based in Chicago, Illinois, and Tucson, Arizona."). Notably, two years after publishing its report, Equifax announced that it had suffered its own massive data breach, affecting more than 147 million consumers. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295 (N.D. Ga. 2019).

[28] Identity Theft Resource Center, "2022 Consumer Impact Report," found at https://www.idtheftcenter.org/wp-content/uploads/2022/09/2022-Consumer-Impact-Report_V3.4_Final_Linked.pdf (last visited November 14, 2022); *see also* Maria Bada & Jason R.C. Nurse, *The Social and Psychological Impact of Cyber-Attacks* (2020), available at https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf (last visited November 14, 2022).

[29] CNBC, "Here's what it costs to freeze your credit after Equifax breach," found at https://www.cnbc.com/2017/09/15/heres-what-it-costs-to-freeze-your-credit-after-equifax-breach.html (last visited November 14, 2022).

monitoring one's credit,[30] and obtaining identity theft prevention services.[31] All of these steps require the expenditure of time and money from individuals whose data was stolen. This includes deciding which of these preventive measures are appropriate, shopping for the best deal, and, over time, monitoring whether the measures are effective and whether one is getting his or her money's worth. Even if one does not ultimately bear the out-of-pocket costs, being a victim of a data breach requires additional time and effort on an ongoing basis, to regularly check one's financial accounts for evidence of identity theft. Indeed, regardless of whether identity theft actually occurs, merely having one's information included in a data breach creates a significant time investment for the victim, which can require many hours and extend over a long period of time.

[30] CNBC, "How much does credit monitoring cost?," found at https://www.cnbc.com/select/how-much-does-credit-monitoring-cost/ (last visited November 14, 2022); Forbes, "Best Credit Monitoring Services Of November 2022," found at https://www.forbes.com/advisor/credit-score/best-credit-monitoring-services/ (November 14, 2022).

[31] Forbes, "Best Identity Theft Protection Services Of November 2022," found at https://www.forbes.com/advisor/personal-finance/best-identity-theft-protection-services/ (last visited November 14, 2022); CNBC, "Spot fraud fast with identity theft protection services that offer up to $1 million in insurance," found at https://www.cnbc.com/select/best-identity-theft-protection-services/ (last visited November 14, 2022).

II. THE UNAUTHORIZED ACCESS OF THEIR INFORMATION GIVES ALL OF THE CLASS MEMBERS STANDING, REGARDLESS OF WHETHER THEY WERE REIMBURSED FOR THEIR HOTEL STAY.

Companies like Marriott and Accenture that undertake to aggregate, store, use, and disseminate users' sensitive personal data take on a grave responsibility, because when information about consumers is accessed without their authorization, they face real-world, concrete harms. Whether tangible or intangible, these harms fit well within the scope of common law harms long recognized by courts as a basis for Article III standing, even if the specific context is more modern.

For this reason, Appellants' attempt to conflate the front-end Article III injury-in-fact inquiry with the later damages inquiry, and thereby escape culpability for their own negligence, is dangerous. It also is unmoored from either traditional common law concepts or common sense, much less from the reality of modern American life. Although the District Court did not abuse its discretion by narrowing the class in response to Appellants' arguments about ascertainability, it does not matter for standing purposes whether Marriott's customers were reimbursed for their hotel stays. Each customer has standing by virtue of the injury caused by the unauthorized accessing of their personal information. As demonstrated below, the loss of privacy and control that results from disclosure of an individual's personal information, in and of itself, is a concrete injury sufficient to confer Article III standing. Whether a Plaintiff or class member bore the economic burden of paying

for a hotel room, and on that basis can ultimately recover damages, is not relevant to and should not be conflated with injury-in-fact for purposes of standing.

American law has historically recognized causes of action for the loss of control over what other people know about us in the form of causes of action for intrusion upon seclusion and other privacy torts. As Warren and Brandeis observed in their seminal work from 1890: "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual … the right 'to be let alone' … Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, Harvard L. Rev. Vol. 4, No. 5. (Dec. 15, 1890) at 195.[32] Warren and Brandeis described intrinsic privacy harms as "a legal injury" or "act wrongful in itself" because it violated the dignity and autonomy of the harmed person. *Id.* This intrinsic privacy harm is distinct from downstream mental, reputational, or pecuniary harms.

The Supreme Court in 1989 confirmed this sentiment: "Information privacy requires the individual's control of information concerning [their] person." *DOJ v. Reporters Committe*e, 489 U.S. 749, 763 (1989). Thus, the mere breach of data—the

[32] Available at https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (last visited November 14, 2022).

release of information from individual control to the wilds of the Internet with its massive and unseen data collection, pooling, and analysis—is sufficient for Article III standing purposes. The loss of control is complete upon release, regardless of the various sorts of damages that might emerge later.

The Supreme Court's recent decisions on Article III standing—*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) and *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021)—support the principle that the unauthorized access of personal information is a concrete harm that gives data breach victims Article III standing to seek redress for that harm, regardless of the financial impact of the disclosure.

In *Spokeo* and *Transunion* the Supreme Court addressed Article III in the context of data that was not breached, but in each case, the Court expressly stated that standing was appropriate when the data was shared outside the platform.

In *Spokeo*, the Supreme Court expressly recognized that both intangible injuries and risks of future harms can satisfy Article III standing. 578 U.S. at 340-41. A key portion of this analysis was grounded in the fact that such injuries were recognized by traditional common law. The Court instructed: "Because the doctrine of standing derives from the case-or-controversy requirement, and because that requirement in turn is grounded in historical practice, it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American

courts." *Id.* at 340-41. Thus, for claims traditionally recognized at common law such as trespass, standing is sufficiently "concrete" at the moment of breach of someone's property, regardless of the nature or amount of damages suffered. As Justice Thomas explained further in his concurrence:

> Common-law courts imposed different limitations on a plaintiff's right to bring suit depending on the type of right the plaintiff sought to vindicate. Historically, common-law courts possessed broad power to adjudicate suits involving the alleged violation of private rights, even when plaintiffs alleged only the violation of those rights and nothing more. "Private rights" are rights "belonging to individuals, considered as individuals." "Private rights" have traditionally included rights of personal security (including security of reputation), property rights, and contract rights. In a suit for the violation of a private right, courts historically presumed that the plaintiff suffered a de facto injury merely from having his personal, legal rights invaded. Thus, when one man placed his foot on another's property, the property owner needed to show nothing more to establish a traditional case or controversy. Many traditional remedies for private-rights causes of action—such as for trespass, infringement of intellectual property, and unjust enrichment—are not contingent on a plaintiff's allegation of damages beyond the violation of his private legal right.

Id. at 344-45 (internal citations omitted).

In *TransUnion*, the Supreme Court again affirmed this historical standard for Article III standing: "Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." 141 S. Ct. at 2204. Similar to *Spokeo*, the Court in *TransUnion* was called to

consider whether a technical violation of a federal statute that protects consumers' personal information—the Fair Credit Reporting Act ("FCRA")—could be a concrete harm for Article III standing purposes. The defendant violated the FCRA by including information in more than 8,000 individuals' credit reports that inaccurately identified them as serious criminals and security threats. *Id.* at 2202.

The Court, relying upon a "close relationship" between FCRA and the tort of defamation, found that publication was necessary to establish harm resulting from the FCRA violation. *Id.* at 2208. For those members of the class whose information had not been disclosed to third parties, the Court rejected standing based on "intangible" harms and the "risk of future harms,", i.e., the mere existence of inaccurate data about a person in a database that had not been disclosed. But importantly, the Court held that those individuals' whose inaccurate personal information had actually been disclosed to third parties outside the company had standing to pursue their FCRA claims. Thus, where the information was disclosed and made available outside the defendant's database, the injury-in-fact was complete upon publication. *Id.* at 2208-09.

Here, the most analogous common law tort for the disclosure of personal information in the Marriott data breach (other than the actual tort of negligence pled) is the tort of disclosure of private information. This tort does not require subsequent damages. Indeed, in the wake of *TransUnion*, multiple courts have held that

plaintiffs had Article III standing based solely on the disclosure of private information, which causes harm regardless of whether the plaintiffs could demonstrate actual damages.

In a case alleging the defendant violated the Stored Communications Act ("SCA") through unauthorized access of the plaintiff's business software account, the Tenth Circuit analogized the harm prohibited by the SCA to "other traditional harms" such as invasion of privacy. *Seale v. Peacock*, 32 F.4th 1011, 1020-21 (10th Cir. 2022). The court held that "[t]he protection of privacy rights does not require a showing of actual damages," and that "the Supreme Court has recognized these invasions of privacy as concrete harms for purposes of standing." *Id.* at 1021(citing *Alvarado v. KOB-TV, L.L.C.*, 493 F.3d 1210, 1217 (10th Cir. 2007) and *TransUnion*, 141 S. Ct. at 2204). The court found the plaintiff had sufficiently alleged an injury-in-fact based on the unauthorized access of his information because, "[e]ven assuming [he] has not alleged actual damages caused by that unauthorized access, the harms stemming from [his] allegations are closely connected to the harms protected by traditional privacy claims where the unauthorized access is itself actionable." *Id.*

Similarly, the Seventh Circuit held that a plaintiff alleged a concrete injury sufficient for Article III standing where her employer unlawfully collected her fingerprint scan and transmitted it to a third-party vendor for authentication in order

to access its computer system. *Cothron v. White Castle System, Inc.*, 20 F.4th 1156, 1161 (7th Cir. 2021). The employer did not obtain her consent before collecting and disseminating her fingerprint scan, in violation of the Illinois Biometric Information Privacy Act ("BIPA"). The court reasoned that the unauthorized disclosure of biometric information, like its undisclosed collection, "amounts to an invasion of an individual's 'private domain, much like an act of trespass.'" *Id.* Because "the failure to obtain consent for a disclosure or dissemination deprives a person of the opportunity to consider who may possess his biometric data and under what circumstances, … [i]t follows that a [BIPA] violation … inflicts a concrete and particularized Article III injury." *Id.*

In *Pratt v. KSE Sportsman Media, Inc.*, 586 F. Supp. 3d 666, 668 (E.D. Mich. 2022), magazine subscribers alleged the publisher violated the Michigan Preservation of Personal Privacy Act ("PPPA") by disclosing their "'Private Reading Information' to several data miners that 'disclosed their information to aggressive advertisers, political organizations, and non-profit companies,' leading to 'a barrage of unwanted junk mail.'" The district court held that "*TransUnion* reinforces that Plaintiffs' PPPA claims have Article III standing," regardless of whether the plaintiffs suffered actual damages. *Id.* at 677. "Accordingly, though Plaintiffs' PPPA claim does not arise from a personal injury or any actual damages, Defendant's violation of the PPPA, assumed true, violated Plaintiffs' statutorily conferred right

to privacy in their reading habits—an intangible harm presenting ample constitutional mooring for Article III purposes." *Id.; accord Hopper v. Credit Associates, LLC*, No. 2:20-cv-522, 2022 WL 943182 (S.D. Ohio Mar. 29, 2022) (recognizing that "[c]ourts have traditionally provided an avenue of relief for alleged violations of privacy" in finding injury-in-fact requirement satisfied).[33]

Courts have reached similar conclusions in data breach cases. In *In re American Medical Collection Agency, Inc. Customer Data Breach Security Litig.*, No. 19-md-2904, 2021 WL 5937742 (D.N.J. Dec. 16, 2021), millions of patients' sensitive information was disclosed when an unauthorized user gained access to the database of a collections vendor hired by the defendant healthcare providers. The district court, resolving the defendants' Rule 12(b)(1) challenge, observed that for purposes of Article III standing, "the unauthorized disclosure of personal information itself constitutes 'a clear de facto injury'" because "'the unauthorized dissemination of personal information' causes 'an injury in and of itself—whether or not the disclosure of that information increase[s] the risk of identity theft or some

[33] *See also, e.g., Desue v. 20/20 Eye Care Network, Inc.*, No. 21-CIV-61275-RAR, 2022 WL 796367, at *2 (S.D. Fla. Mar. 15, 2022) ("Concrete intangible harms may include reputational harms, disclosure of private information, and intrusion upon seclusion."); *Ruk v. Crown Asset Mgmt., LLC*, No. 1:16-CV-3444-LMM-JSA, 2017 WL 3085282 (N.D. Ga. Mar. 22, 2017) ("This consideration also strongly supports the finding of a concrete injury, because our common law traditionally recognizes a right of individual privacy, which is legally protected by the courts in certain circumstances.").

other future harm." *Id.* at *7 (quoting *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 626, 629 (3d Cir. 2017)). The court further recognized that "[a]n unauthorized 'disclosure of private information' is" one of the "intangible harms … sufficiently 'concrete' to establish an injury in fact." *Id.* at *9. Noting that "[a] plaintiff who suffers a wrongful disclosure need not additionally demonstrate misuse resulting in economic harm," the court found that plaintiffs alleging solely intangible harms "alleged a concrete and particularized intangible injury arising from the intrusion upon their privacy interests following the alleged wrongful access and misuse of their Personal Information." *Id.*

In *Wynne v. Audi of America*, No. 21-cv-08518-DMR, 2022 WL 2916341 (N.D. Cal. Jul. 25, 2022), the plaintiff, seeking to have her case remanded to state court after removal to federal court, argued that she lacked Article III standing because she had not alleged a "concrete harm" stemming from a data breach. *Id.* at * 2. But the district court, applying *TransUnion*, rejected her argument. The court held that the invasion of her privacy interests that occurred as the result of the data breach "is a concrete injury that establishes Article III standing" because "'disclosure of private information' is an intangible harm that is 'traditionally recognized as providing a basis for lawsuits in American courts.'" *Id.* at *5 (quoting *TransUnion*, 141 S.Ct. at 2204).

Most recently, in *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022), the Third Circuit explained that "[i]n the data breach context, there are several potential parallels to harms traditionally recognized at common law, depending on the precise theory of injury the plaintiff puts forward. For example, if the theory of injury is an unauthorized exposure of personally identifying information that results in an increased risk of identity theft or fraud, that harm is closely related to that contemplated by privacy torts that are 'well-ensconced in the fabric of American law.'" *Id.* at 154-55 (quoting *In re Horizon*, 846 F.3d at 638-39); *see also Leonard v. McMenamins, Inc.*, No. 2:22-cv-00094-BJR, 2022 WL 4017674, at *4-5 (W.D. Wash. Sept. 2, 2022) ("Nevertheless, Plaintiffs have alleged an injury-in-fact based not on the risk of future identify fraud created by the data breach, but on the actual harm resulting from the theft of Plaintiffs' PII itself."); *In re USAA Data Sec. Litig.*, No. 21 CV 5813 (VB), 2022 WL 3348527, at *4 (S.D.N.Y. Aug. 12, 2022) (finding the loss of privacy arising out of a data breach that disclosed plaintiffs' driver's license number was sufficient to plausibly allege injury-in-fact).

The holdings of these cases are equally applicable here. Plaintiffs and each class member suffered actual harm as a result of the loss of privacy and control of their personal information at the moment of the Marriott data breach. This is sufficient injury-in-fact for Article III standing and also constitutes common injury for class certification purposes. The current class definitions, as revised by the

District Court, do not cause the ascertainability problems suggested by Appellants. But if this Court finds otherwise, it should solve that ascertainability problem by modifying the class definitions to include every customer who paid Marriott and whose information was disclosed in the Data Breach, as each of them has standing.

CONCLUSION

The District Court's certification order should be affirmed.

Dated: November 22, 2022

Respectfully submitted,

/s/ Jean Sutton Martin

Jean Sutton Martin
John A. Yanchunis
Kenya J. Reddy
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g)), I certify the following:

This brief complies with the type-volume limitation of Rules 32(a)(7)(B) and 29(a)(5) of the Federal Rules of Appellate Procedure because this brief contains 5,208 words, excluding the parts of the brief exempted by Rule 32(f) of the Federal Rules of Appellate Procedure.

The brief complies with the with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word in Times New Roman, 14 point font.

Dated: November 22, 2022

/s/ Jean Sutton Martin
Jean Sutton Martin

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on November 22, 2022, I electronically filed a true and correct copy of the foregoing brief with the Clerk of the Court using the CM/ECF system, which will send notification to all attorneys of record in this matter.

/s/ Jean Sutton Martin
Jean Sutton Martin